Estruturas Algébricas I

Natanael Oliveira Dantas

São Cristóvão/SE
2009

Sumário

Aula 01

A ESTRUTURA DE DOMÍNIO ORDENADO DOS NÚMEROS INTEIROS

META

Discutir as principais propriedades da estrutura de domínio bem ordenado dos números inteiros.

OBJETIVOS

Ao final desta aula, o aluno deverá:

Aplicar as propriedades da estrutura de domínio dos inteiros na demonstração de outras proposições decorrente destas.

Aplicar o princípio de indução na resolução de problemas referentes a números naturais.

PRÉ-REQUISITOS

O pré-requisito para esta aula é o curso de Fundamentos de Matemática. Portanto, disponibilize as aulas impressas desta disciplina e as consulte sempre que você necessite.

INTRODUÇÃO

Seja bem-vindo, prezado aluno! Esta aula é o início da nossa jornada rumo ao universo das estruturas algébricas.Tradicionalmente, a matemática divide-se em três grandes áreas: a Álgebra, a Análise e a Geometria/Topologia. Entretanto, tal tricotomia está cada vez mais se descaracterizando tanto pelo aparecimento de outros segmentos que não se encaixam unicamente em uma destas quanto pela necessidade de novas técnicas. Outro fator é a interface entre áreas dando origem a novas teorias. Por exemplo, topologia algébrica é a interface entre álgebra e topologia. É importante que você, futuro professor, tenha uma boa preparação em cada uma destas áreas e, este é o primeiro dos dois cursos de Álgebra dos currículos dos cursos de Matemática da UFS.

A palavra Álgebra vem de um manuscrito árabe de cerca de 800 a.C., que estabelece leis para a resolução de equações e, até a segunda metade do século XIX, a Álgebra era vista apenas como uma teoria de equações. Atualmente, a álgebra é mais do que isto; trata-se da área da Matemática que lida com conjuntos munidos de operações e relações formais chamados estruturas algébricas. É uma coleção de modelos abstratos provindos até mesmo de outras áreas da Matemática e ciências afins.

Os objetos da Álgebra são classificados de acordo com os tipos de operações que neles podem ser efetuadas e pelas propriedades das quais gozam tais operações. Grupos, anéis, ideais, espaços vetoriais, módulos e corpos são exemplos de como um conjunto pode ser estruturado algebricamente.

Em regra, um primeiro curso de Álgebra trata das estruturas de grupos e anéis. Deste modo, são estes os conteúdos presentes neste curso. Nas três primeiras aulas apresentaremos informalmente os números inteiros e discutiremos suas primeiras propriedades. Tal abordagem servirá de modelo no estudo de grupos e anéis.

A ESTRUTURA DE DOMÍNIO DOS INTEIROS

No conjunto $\mathbb{Z}$ dos inteiros estão definidas a adição e a multiplicação. Tais operações satisfazem as seguintes propriedades:

i) Associativa da adição. $\forall$a,b $\in \mathbb{Z}$, $(a+b)+c=a+(b+c)$.

ii) Comutativa da adição. $\forall a,b \in \mathbb{Z}$, $a+b=b+a$.

iii) Existência do elemento neutro para a adição. Existe em $\mathbb{Z}$, o zero, tal que $a^{'}+0=a$, para todo $a \in \mathbb{Z}$.

iv) Existência do oposto. Para cada $a \in \mathbb{Z}$ existe $-a \in \mathbb{Z}$ tal que $a+(-a)= 0$.

v) Distributiva da multiplicação em relação à adição. $\forall a,b,c \in \mathbb{Z}$, $a.(b+c)=a.b+a.c$ e $(a+b).c=a.c+b.c$.

vi) Associativa da multiplicação. $\forall a,b \in \mathbb{Z}, (a.b).c=a.(b.c)$.

vii)Comutativa da multiplicação. $\forall a,b \in \mathbb{Z}, a.b=b.a$.

viii) Existência do elemento neutro para a multiplicação. Existe em $\mathbb{Z}$, o um, $(1 \neq 0)$, tal que, $a.1=a$, para todo $a \in \mathbb{Z}$.

ix) Integridade. Se $a,b \in \mathbb{Z}$ e $a.b=0$ então $a=0$ ou $b=0$.

Futuramente, na aula 10, estudaremos os anéis que são estruturas algébricas das quais o conjunto dos números inteiros munido das operações adição e multiplicação verificando às cinco primeiras propriedades aqui exibidas, é um exemplo. Os inteiros munidos destas operações verificando às oito primeiras propriedades é chamado um anel comutativo com identidade e como verifica também a nona è chamado um domínio de integridade.

Definição 1. Nos inteiros, definimos a diferença entre dois elementos $a \; e \; b$, (nesta ordem), como sendo o inteiro $a - b = a + \; (-b)$.

Decorrem da estrutura de domínio de integridade dos inteiros as propriedades contidas na Proposição 1.

i) Os elementos neutros 0 e 1 são únicos.

ii) Cada inteiro tem um único oposto.

iii) $\forall \; a \in \mathbb{Z}, a\,.0 = 0$.

iv) $\forall a, b \in \mathbb{Z}, (-a).\,b = a\,.\,(-b) = \; -(a.\,b)$.

Demonstração. i) Se existissem $0, 0^{'} \in \mathbb{Z}$ tais que para cada $a \in \mathbb{Z}, a + 0 = a + 0^{'} = a$ então, em particular, teríamos

$0^{'} + 0 = 0'$ e $0 + 0^{'} = \; 0$ e da comutatividade da adição, $0 = 0'$. Portanto, o elemento neutro da adição é único.

A demonstração da unicidade do elemento neutro da multiplicação é análoga à, feita acima e deixaremos como atividade.

ii) Dado $a \in \mathbb{Z}$, suponhamos que existam $b, c \in \mathbb{Z}$ tais que $a + b = a + c = 0$. Podemos escrever: $b = b + 0 = b + (a + c) = (b + a) + c = (a + b) + c = 0 + c = c$ donde segue a unicidade.

iii) Dado $a \in \mathbb{Z}$ notemos que $a\,.0 = a\,.\,(0 + 0) = a.\,0 + a.\,0$. segue que $a.\,0$ e $a.\,0 + a.\,0$ têm o mesmo oposto $-(a.\,0)$ logo, $-(a.\,0) + a.\,0 = -(a.\,0) + (a.\,0 + a.\,0)$ donde temos que $a.\,0 = 0$.

iv) Vamos provar que $(-a).\,b = -(a.\,b)$. Com efeito, notemos que $(-a).\,b + ab = \big((-a) + a\big).\,b = 0.\,b = 0$. Segue que $(-a).\,b$ é um oposto de $a.\,b$. Da unicidade do oposto, temos que $(-a).\,b = -(a.\,b)$.

O caso $a.\,(-b) = -(a.\,b)$ é semelhante e deixaremos como atividade.

A BOA ORDENAÇÃO DE $\mathbb{Z}$.

Em $\mathbb{Z}$ existem a relação de ordem total $\leq$ e o conceito de valor absoluto $|\;|$, que admitiremos com suas propriedades básicas visando estabelecer resultados futuros. Neste sentido vamos assumir inicialmente o principio da boa ordem.

Principio da boa ordem: Todo subconjunto não vazio A de $\mathbb{Z}$ de elementos não negativos $(de\;\mathbb{N})$ possui elemento mínimo.

Exemplo 1. Para $A = \{5,8,11,14\}, m\acute{\imath}n(A) = 5$.

Proposição 2. Não existe inteiro a tal que $0 < a < 1$.

Demonstração: Suponhamos que exista um a inteiro tal que $0 < a < 1$. Então o conjunto $S = \{a \in \mathbb{Z} : 0 < a < 1\}$ é não vazio e do princípio da boa ordem existe $a_0 = m\acute{\imath}n(S)$. Como $a_0 \in S$ segue que $0 < a_0 < 1$ donde temos que $0 < a_0^2 < a_0 < 1$, contradizendo a minimalidade de a_0.

Proposição 3. (Indução – 1ª forma) Seja S uma sentença aberta sobre N para a qual valem:

i) $S(0)$ é verdadeira;

ii) Se $a \in \mathbb{N}\ e\ S(a)$ é verdadeira então $S(a+1)$ é verdadeira.

Portanto, $S(a)$ é verdadeira para todo a pertencente a $\mathbb{N}$.

Demonstração: Seja A o conjunto dos inteiros não negativos para os quais $S(a)$ seja falsa, e suponhamos que $A \neq \phi$. Do princípio da boa ordem existe $a_0 = m\acute{\imath}n(A)$. Segue de i) que $a_0 \geq 1$, isto implica que $a_0 - 1 \notin A$ donde segue que $S(a_0 - 1)$ é verdadeira. Finalmente por ii) temos que $S(a_0) = S((a_0 - 1) + 1)$ o que é uma contradição. Portanto $S = \phi$ e a demonstração está concluída.

Proposição 4**.** (Princípio de indução – 2ª forma). Seja S uma sentença aberta para a qual valem:

i) $S(0)$ é verdadeira;

ii) Para cada $a \in \mathbb{N}, a \neq 0, S(b)$ é verdadeira para $1 \leq b < a$ implica $S(a)$ verdadeira.

Então $S(a)$ é verdadeira para todo $a \in \mathbb{N}$.

Demonstração**:** Se esta proposição não fosse verdadeira, então existiriam uma sentença aberta S sobre $\mathbb{N}$, verificando i) e ii) e um $a \in \mathbb{N}$ para a qual $S(a)$ seria falsa. Supondo a o menor natural com tal propriedade, então $a > 0$ e $\forall b \in \mathbb{N}$ com $0 \leq b < a$, $S(b)$ seria verdadeira. Por "ii)", $S(a)$ seria verdadeira, uma contradição.

Observação: Não é difícil perceber que nas proposições 6 e 7, o domínio da sentença abertas S pode ser um conjunto do tipo $\{a_0, a_0 + 1, a_0 + 2, \dots\}$ onde a_0 é um inteiro pré-fixado.

Definição 2. Dados $a \in \mathbb{Z}\ e\ n \in \mathbb{Z}_+, definimos$ a potência de base a e expoente n, pondo

$$a^n = \begin{cases} 1 & se \quad n = 0 \\ a.a^{n-1} & se \quad n > 0 \end{cases}$$

Exemplo 1.2.2. $a^1 = a.a^{1-1} = a.a^0 = a\,.1 = a$

$a^2 = a.a^{2-1} = a.a$

$a^3 = a.a^2 = a.a.a.$

Exemplo 3. Para cada $n \in \{2,3,\dots\}$, vamos usar o princípio de indução para provar que $1 + 3 + \cdots + (2n - 1) = n^2$. Notemos que para $n = 2$, temos $1 + 3 = 2^2$ e, a expressão é verdadeira. Admitamos agora, por hipótese, que para $n \geq 2$ a expressão acima é verdadeira e, vamos provar que isto implica na veracidade da expressão para $n + 1$. Com efeito, $1 + 3 + \cdots + (2(n+1) - 1) = 1 + 3 + \cdots + (2n - 1) + (2(n+1) - 1) = n^2 + (2(n+1) - 1 = n^2 + 2n + 1 = (n+1)^2$. Portanto, a expressão acima é verdadeira $\forall n \in \{2,3,\dots\}$.

Exemplo 4. Usando indução, vamos provar que $a^m.a^n = a^{m+n}$ $\forall a \in \mathbb{Z}$ e $\forall m, n \in \mathbb{Z}_+$. Para tal, caro aluno, vamos escolher um entre m e n, para usar indução, digamos n e fixar a e m (embora arbitrários). Com efeito, para $n = 0$, temos $a^m.a^0 = a^m.1 = a^m$ e $a^{m+0} = a^m$. Logo , $a^m.a^0 = a^{m+0}$ ok! Suponhamos agora, por hipótese que $a^m.a^n = a^{m+n}$ e vamos olhar para $a^m.a^{n+1}$. Ora, por definição, $a^{n+1} = a.a^{(n+1)-1} = a.a^n$, logo, $a^m.a^{n+1} = a^m(a.a^n) = a^m.(a^n.a) = (a^m.a^n).a = a^{m+n}.a = a.a^{m+n} = a^{(m+n)+1} = a^{m+(n+1)}$

Resumindo: para $a \in \mathbb{Z}$ e $m \in \mathbb{Z}_+$ arbitrários, a propriedade é válida para $n = 0$ e ser válida para n implica ser válida para $n + 1$. Logo do princípio de indução é válida $\forall n \in \mathbb{Z}_+$. Sendo $a \in \mathbb{Z}$ e $m \in \mathbb{Z}_+$ arbitrários, podemos concluir que a mesma é verdadeira.

Definição 3. O domínio $\mathbb{Z}$, numido da relação de ordem total " $\leq$ " para a qual vale o princípio da boa ordem dá a $(\mathbb{Z}, +, 0, \leq)$ uma estrutura algébrica chamada, domínio bem ordenado.

RESUMO

Nesta primeira aula, aprendemos as primeiras propriedades dos números inteiros onde discutimos sua estrutura de domínio ordenado onde apresentamos os princípios da boa ordem e de indução que serão pré-requisitos fundamentais das próximas aulas.

ATIVIDADES

1. Provar que a única solução em $\mathbb{Z}$ da equação, $x + a = b$, na variável x é $b - a$.

2. Provar que, em $\mathbb{Z}$, as únicas soluções da equação $x^2 = x$ são 0 e 1.

3. Provar que $\forall a \in \mathbb{Z}, a^2 = (-a)^2$

4. Usando o princípio de indução, provar que:

a) $1^2 + 2^2 + \cdots + n^2 = \frac{1}{6} n(n+1)(2n+1), \forall n \in \{2,3,\dots\}$.

b) $n < 2^n,\ \forall n \in \mathbb{N}$.

COMENTÁRIOS DAS ATIVIDADES

Caro aluno, se você aprendeu as propriedades da estrutura de domínio dos inteiros em especial a existência e unicidade do oposto de cada inteiro e integridade então você resolveu corretamente as primeira e segunda atividades.

Na terceira atividade você deve ter usado o item iv) da proposição 1.

Na quarta atividade, para resolvê-la, você deve ter aplicado indiretamente algumas das nove propriedades da estrutura de domínio e ter aprendido que na aplicação do princípio de indução, testa-se a veracidade da sentença aberta no primeiro elemento do conjunto, assume que a mesma é verdadeira para um elemento genérico do conjunto e com esta hipótese justifica que a mesma é verdadeira também para o sucessor deste elemento, concluindo finalmente que a sentença é verdadeira para todos os elementos do conjunto em apreço.

REFERÊNCIAS

GONÇALVES, Adilson. Introdução à álgebra. 5. ed. Rio de Janeiro: IMPA, 2007. 194 p. (Projeto Euclides) ISBN.

HUNGERFORD, Thomas W. Abstract algebra: an introduction. 2nd. ed. Austrália: Thomson Learning, ©1997.

GARCIA, Arnaldo; LEQUAIN, Yves. Elementos de algebra. 3. ed. Rio de Janeiro: IMPA, 2005. 326 p. (Série: Projeto Euclides).